2004 Command and Control Research and Technology Symposium
The Power of Information Age Concepts and Technologies
San Diego, CA 15-17 June 2004

Track 7: Effects Based Operations and Emerging Concepts

Identity Management: Role Based Access Control for Enterprise Services

Rick Kooker, PMP

Stephan Kane, PMP

Science Applications International Corporation

3049 Ualena Street, Suite 1100

Honolulu, Hawaii 96819

(808) 833-8600 (P) (808) 834-0658 (fax)

Email: kookerf@saic.com

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 2004		**00-00-2004 to 00-00-2004**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Identity Management: Role Based Access Control for Enterprise Services	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Science Applications International Corporation,3049 Ualena Street Suite 1100,Honolulu,HI,96819**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**		**30**	

"Effective systems management depends primarily on . . . implementation of policy-based management. You simply cannot count on technology alone to see you through."

Network and Systems Managers' Best Practices Report 2004

ABSTRACT

The current Department of Defense (DoD) Network consists of separate domains, disparate networks that are geographically dispersed, and resourced by hundreds of diverse funding sources. As we move into a Network Centric DoD Enterprise and as Web and data services become available throughout the DoD Network with applications becoming Enterprise wide, an unreasonable burden will be placed on the service providers to research and gather the appropriate data to determine if users requesting access should be authorized that access. A most challenging problem in managing large distributed systems is the complexity of security administration. Since most applications are not yet available as Web Services but rather still controlled within a certain localized command or enclave, the issue of authorization is manageable albeit error prone and expensive. DoD transformation to a Network Centric environment requires robust authentication of users and Web Services for C2 based on PKI/biometric technology and subsequent authorization/Access to data/services/applications provided by an Enterprise Role Based Access Control (ERBAC) system. This paper is designed to convey information to the audience of the importance, necessity, and urgency associated with the problem, the need to commit resources for a solution and subsequently working within that solution across the DoD enterprise.

PROBLEM

The National Institute of Standards and Technology (NIST) defines role-based access as when: "access decisions are based on the roles that individual users have as part of an organization."

This discussion concedes that there are more than a few technically sophisticated and thoroughly operable Identity Management (IdM) solutions fully capable of providing the means to implement a successful Enterprise RBAC. There is no lack of approaches involving Directory Services, hierarchical role inheritance schemas, biometric and Public Key Infrastructure (PKI) authentication standards, Single Sign On (SSO) solutions, Security Assertion Markup Language (SAML) assertions, etc. The actual discussion here is more from the Operational perspective rather than from a Systems or Technical viewpoint.

So far, most of the basic RBAC development efforts have been initiated and supported by the DoD. In the past DoD requirements were primarily aimed at preventing the unauthorized access to classified information, and now more recently, the commercial world has become involved due to Privacy Act concerns, Health Insurance Portability and Accountability Act (HIPAA) patient record confidentially, liabilities, and the increased cost of systems administration.

There are two fundamental types of access control: Discretionary Access Control (DAC) and Mandatory Access Control (MAC). DAC permits the granting and revoking of access control privileges to be left to the discretion of the individual users or organizations. A DAC mechanism allows users to grant or revoke access to any of the systems/applications under their control. DAC is normally implemented based on some locally (individual data owner or organization) determined formula derived from some combination of data ownership and the requesting individuals job functions that might require access to that data. MAC, as defined in the DoD's Trusted Computer Security Evaluation Criteria (TCSEC), is "A means of restricting access to objects based on the sensitivity (as represented by a label) of the information contained in the objects and the formal authorization (i.e. clearance) of subjects to access information of such sensitivity." The current DoD Enterprise Access Control schema seems to reflect a somewhat arbitrary blend of DAC/MAC loosely overlying the "rugged individualism" as currently practiced within each of the branches of Services in DoD.

In the past, the pre-Network Centric Enterprise Services (NCES) DoD C2 and Information Management (IM) environment was defined by sheer distances, "trusted" systems, large

organizational structures with very vertical and limited Communities of Interest/Communities of Practice (COI/COPs), centralized decision making processes with relatively few decision makers, and a limited availability of timely data, all of which mandated an environment populated by relatively static "roles" for participants, particularly in terms of geographic location and organization.

Even today's DoD Enterprise Network is still primarily one of separate domains/enclaves, disparate networks that are geographically dispersed and are resourced by a multitude of diverse funding sources/services. The limiting factor in our Network Centric Warfare Operation is now complexity, not lack of bandwidth, computing power, or timely data as in the past. This Transformational technology is rapidly forcing all of us into a Network Centric DoD Enterprise based on Web based technology characterized by "death to distance", rapid acquisition of vast amounts of timely information, very extensive COIs/COPs, and transition to a Service Oriented Architecture (SOA). There is already a growing litany of IM innovations occurring as Transformation gains momentum throughout the DoD.

As customers on the DoD Enterprise become aware of the plethora of the existing applications/services, the System Administrators and Central Design Authorities (CDAs) for those application/services are quickly confronted with an exponential growth in the numbers of prospective users of their applications/services. This phenomenal growth is rarely accompanied with adequate funding or technological refreshment to support the increased base of customers. Some recent efforts such as Army Knowledge Online (AKO), Navy Marine Corps Intranet (NMCI) and Task Force Web (TFWeb) have provided lessons learned and valuable direction for application/data owners on what happens when users increase from thousands to tens or hundreds of thousands and how to construct Web Services and applications to ensure their availability throughout the DoD Enterprise. However, relatively little has been accomplished in the planning for controlling access to those applications/services.

As Web Services become available throughout the DoD Network and applications become Enterprise wide, an unreasonable burden is being placed on the service providers/system administrators to research, gather, and sometimes, verify the appropriate personal/Command data necessary in order to make a determination regarding authorization of a user's request for access. Today, security administration is often costly and prone to error partially because many applications/systems utilize static Access Control Lists (ACLs) to link an individual's access with

each resource on the system by means of "forms based" logins. Despite the growing use of "semi-automated self-sign up registration, email back password" approaches for some applications, the current process for validating users "need to know" is labor intensive, sporadic, error prone, and performed solely by the data/applications/systems owner, CDA, responsible for each user access request. Rarely, if ever, are users forced to update USERIDs or passwords on DoD systems. So, when granted access to an application/system, the user usually ends up having access "forever", despite possible subsequent alterations of his/her "need to know", level of security clearances, retirement from DoD, etc. In the case of one of the authors, it was surprising to discover that access on one of the Navy's Portals, had never been altered despite a substantial change in personnel status. Even when an application/system is controlled within a localized command network or enclave, the management authorization process is challenging and often fails in an operational scenario. There is evidence that a strong contributing factor in many "blue on blue" engagements is that the decision support operator often has either no knowledge of, and/or access to pertinent information/data held in another system.

As the prospective customer base grows exponentially and more of our thousands of applications/systems become available on an enterprise level, continued use of current processes/methodologies to enable users access on an individual basis will be overwhelmed and the most important limitation of our C2 system's success will now become access control rather than bandwidth, operability, or survivability.

SOLUTION

Simply put, Network Centric Warfare C2 requires a rapid yet completely trustworthy biometrically enabled Single Sign On (SSO) methodology for Authentication and Authorization/Access Control based on both need-to-know and the role of the individual or group in the process requiring access. This access can no longer be based on relatively static Organizational Command structures but needs to be based on dynamic, process-based Operational/Functional requirements enabling horizontal fusion. *The DoD Enterprise RBAC (ERBAC) must blend people, functions/processes, data, time, location and situation into a simple, widely recognized (including allies); rapidly adaptable, mutually agreed upon model that always ensures correct and successful access for the decision maker.* Any effort to accomplish this will ultimately fail if the best practices and

principles of enterprise architecture frameworks, project management, and business rules management are not used in concert and with the active participation of the operational Joint/Combined military community.

Although it is not intended in this paper to go into detail about the plethora of commercial or government developed tools that allow ERBAC to be used, it is worth noting that the National Institute of Standards and Technology has issued an American National Standard on Role Based Access Control - ANSI INCITS 359-2004 (approved 19 Feb 2004). In addition, within OASIS, the XACML technical committee is developing an RBAC profile for expression of authorization policies in XML, making it easier to build RBAC into web applications. Web applications can use RBAC services defined by the OASIS XACML Technical Committee.

A significant amount of effort has been expended by several companies to craft RBAC solutions for their enterprise-focused customers. Some representative tools and companies include Computer Associates' eTrust tool suite, SYSTOR AG's Sam Jupiter, Netegrity's Business Layers Day One software (which can take input directly from human resources applications to generate requests for new user accounts for application resource access), and OpenNetworks' Directory Smart provisioning software in conjunction with Microsoft's Active Directory. In addition, several companies have developed solutions in-house, such as Chevron, Anthem Blue Cross/Blue Shield, and State Farm. Many of these solutions are being implemented in conjunction with provisioning efforts as new network hardware and software is introduced.

A detailed discussion of an adaptation of the CA eTrust suite to a DoD application is contained in the paper contributed by Richard Fernandez to the C4ISR/C2 Architecture track to the 2004 CCRTS Conference.

APPROACH

To state the obvious, adequately resourcing the required cultural and process change in the DoD coincident with and mutually supportive of the move to Network Centric Warfare is the first imperative. The task of determining the ‘who, what, how, where, when and why’ of ERBAC is not a technical issue, but an operational one.

Under the NCES model, interoperability is no longer optional so the inclusion of provisions for a functional ERBAC is mandatory when designing and fielding complex technical Joint systems.

- ERBAC should be added to the nine (9) Core Enterprise Services currently listed for NCES.
- DoD should fund and maintain a DoD ERBAC office as part of the GIG Enterprise Architecture (EA) effort with an ERBAC representative at every major Joint and Service Echelon 2 and above Command. The ERBAC must be one of the major pillars of the Operational portion of the C4ISR Enterprise Architecture. The purpose would be to collaborate on requirements and "socialize" possible solutions rapidly so that a framework can be implemented rapidly DoD wide.
- Current and prospective system owners/users at every echelon level must be tasked and resources provided by DoD. All CDAs, and Systems and Acquisition Commands must be tasked to include an ERBAC matrix for their system Concept of Operations. The process of defining required roles/policies/rules should be based on a thorough analysis of how the end user operates or is planning on operating the system and should include input from a wide spectrum of users (stakeholders) of the system.
- The ERBAC matrix could possibly include:

    1. ***People:***

       Attributes; clearance, rank, unit, status, job, biometric, PKI, Service Branch, DOB, nationality, etc. These should be delineated by the alterability of the attributes. This portion of the IdM/ERBAC must be maintained locally for obvious reasons.

       Assigned roles/rules (e.g., Strike Planning Officer, Intel Analyst, Tactical Action Officer, Disbursing Clerk, Aviation Electronics Technician, Message Releaser, etc.).

    2. ***Functions/Processes/Rules:***

       Identify the description of function, the process/sub processes and data involved and the component action of each process. Identify the desired outcome of every process.

    3. ***Data:***

       Data dictionaries, data elements mapped to above functions, CRUD tables, etc.

4. ***Time:***

   Identify rules/roles based on time, after hours, weekends, 24/7 operations, security badge expiration, etc.

5. ***Situation*:** INFOCON, DEFCON, FPCON, "Weapons Free", Rules of Engagement, etc.

CONCLUSION

Over the past decade, the Department of Defense has made immense investment in information systems infrastructure, applications, and policies. In addition, there are thousands of dedicated IT professionals and C2 operators at work every day, trying to use those assets to the best advantage. The promised return on investment has not been realized in many cases, because there is no unified enterprise architecture and no enterprise business rules. The planning and implementation of an Enterprise Role Based Access Control system is vital to the leveraging the investment and creating real value for the enterprise. The concept of an enterprise is new to many DoD organizations and requires a different approach to information and knowledge management than the current ad-hoc network structures. The technology to create an ERBAC system exists and is being implemented today in several large organizations around the world. The DoD enterprise is highly specialized and decentralized and requires specific enterprise architecture, business rules planning, and accountable project portfolio management. Network Centric C2 capability is essential for current and future operations against ever more wily and technologically knowledgeable adversaries. ERBAC makes enterprise network centric C2 possible. Proper resourcing, organizational analysis, and project and change management are keys to the success of any ERBAC effort.

REFERENCES

Barkley, John and Cincotta, Anthony "Implementation of a Role/Group Permission Using Object Access Type". *U.S. Patent 6202066 B1 (13 Mar 2001)* <http://www.itl.nist.gov/div897/staff/barkley/6202066.pdf>

Cruikshank, Peter and Coxe, David. "Adaptive Identity Management: Market and Requirements Analysis". Unpublished Technical Concept Paper, SAIC, 11 Feb 2004.

Kern, Axel, "Advanced Features for Enterprise-Wide Role Based Access Control." *Proceedings of the 18th Annual Computer Security Application Conference, Las Vegas, Nevada, Dec 2002*

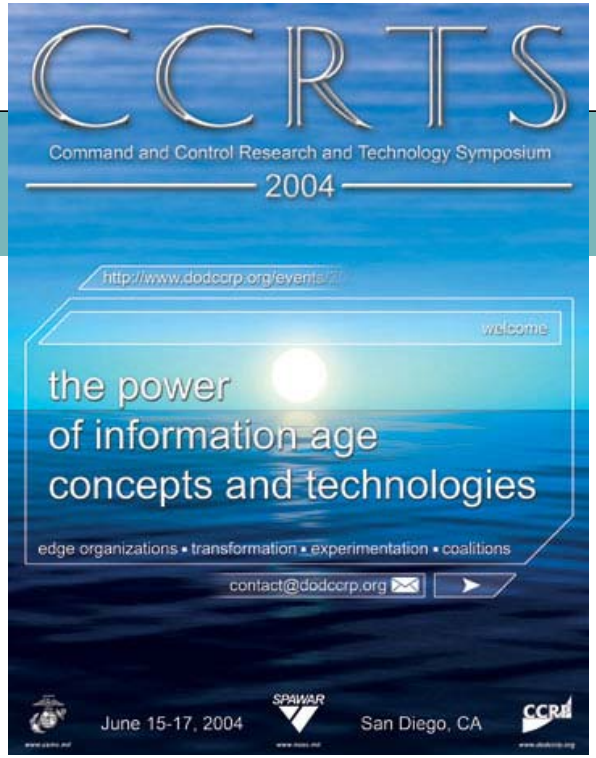
Messmer, Ellen, "Role Based Access Control on a Roll", *Network World, 30 Jul 2001* <http://www.nwfusion.com/archive/2001/123359_07-30-2001.html>

Oh, Sejong and Park, Seog. "Enterprise Model as a Basis of Administration on Role-Based Access Control". *Third International Symposium on Cooperative Database Systems for Advanced Applications (codas) Beijing, China (23-24 Apr 2001)* <http://www.sogang.ac.kr/english>

Sandhu, R., Ferraiolo, D.F., and Kuhn, DR "The NIST Model for Role Based Access Control: Towards a Unified Standard," *Proceedings, 5th ACM Workshop on Role Based Access Control (26-27 Jul 2000)*

"Enabling True Role Based Management" *Eurekify Sage (20 Mar 2004)* <*http://www.eurekify.com/solutions.htm*>

National Institute of Standards and Technology (NIST). "Information Technology-Role Based Access Control American National Standard" *ANSI INCITS 359-2004 (approved 19 Feb 2004)* <http://www.ncits.org/Archive/2004/n251_275.htm>



An Employee-Owned Company

Identity Management: Role Based Access Control for Enterprise Services

16 June 2004

Rick Kooker, PMP

Stephan Kane, PMP

Information Management Evolution

SAIC®
An Employee-Owned Company

- **1960's-1990's Challenges**
  - Lacked bandwidth
  - Lacked computing power
  - Lacked timely access to information
- **2000's Challenges**
  - Data and user overload
  - "BLUE on BLUE" challenge
  - Larger Domains (audiences) with no additional funding (NMCI)
  - Decentralized decision making
  - DoD "Transformation" and "JOINT-ness"

Cyber Identity

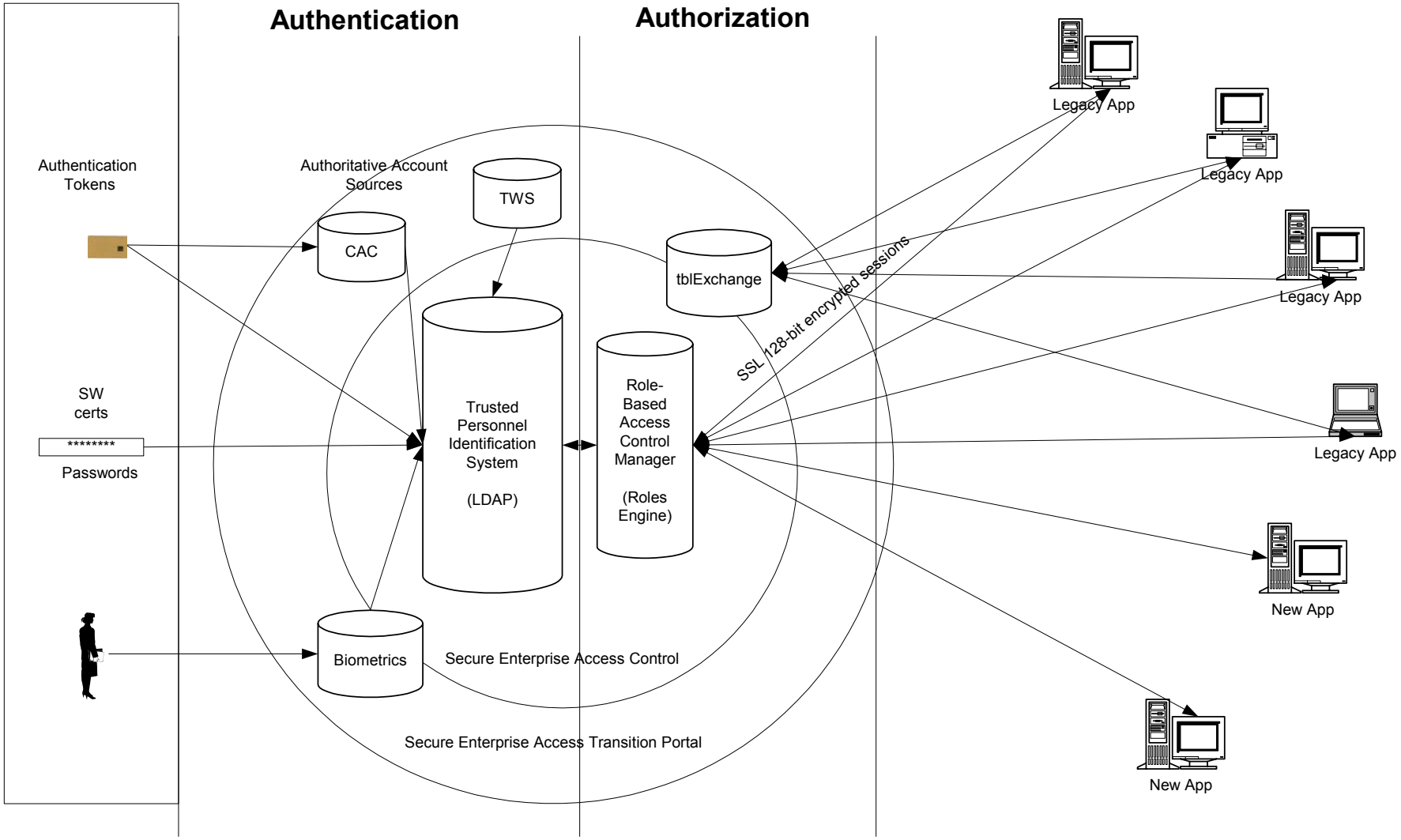
- Critical feature for future of network computing
- Must confirm with confidence
  - Validity of online transactions
  - Identity of individuals involved in those exchanges
- Must precisely verify who you are dealing with online
- Protect against unauthorized access to mission-critical systems and data
- ***Critical for Web Services***

Maintenance of Cyber Identity

An Employee-Owned Company

- Who do I let see my data? Need to Know ?
- Who is accessing my data via Web Services?
- Privacy Act Issues
- Management of relationship of individual user to systems and network and/or Web service

Traditional Architecture



Issues and Challenges

- NIST RBAC Definition
- ID Management Solutions (IdM)
- DoD RBAC Work to Date
- Expanded DoD and Commercial Efforts

Notable Ongoing ERBAC Efforts

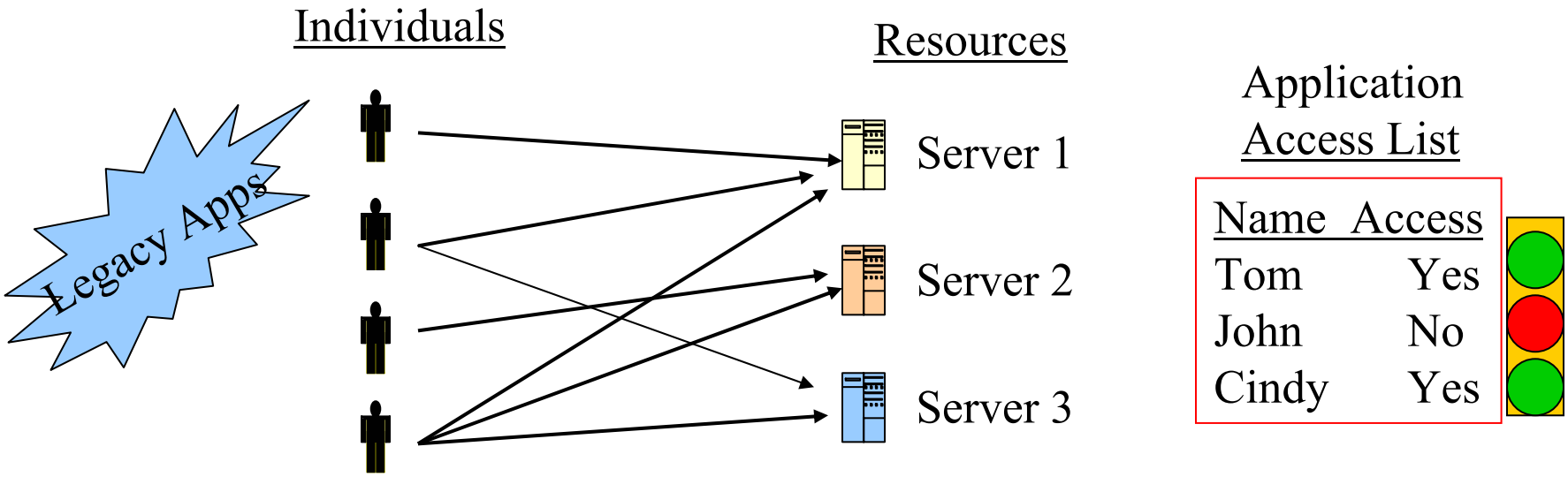
- NIST American National Standard on Role Based Access Control - ANSI INCITS 359-2004 (approved 19 Feb 2004)
- In OASIS, the XACML technical committee is developing an RBAC profile for expression of authorization policies in XML
- Computer Associates' eTrust
- SYSTOR AG's Sam Jupiter
- Netegrity's Business Layers Day One
- OpenNetworks' Directory Smart provisioning software in conjunction with Microsoft's Active Directory
- In-house efforts by Chevron, Anthem Blue Cross/Blue Shield, and State Farm
- Many solutions are being implemented in conjunction with provisioning efforts for new network hardware and software
- Adaptation of the CA eTrust suite to a DoD application is contained in Richard Fernandez' paper 196 for CCRTS

Types of Access Control

- Discretionary (DAC)
- Mandatory (MAC)
- Role-Based (RBAC)

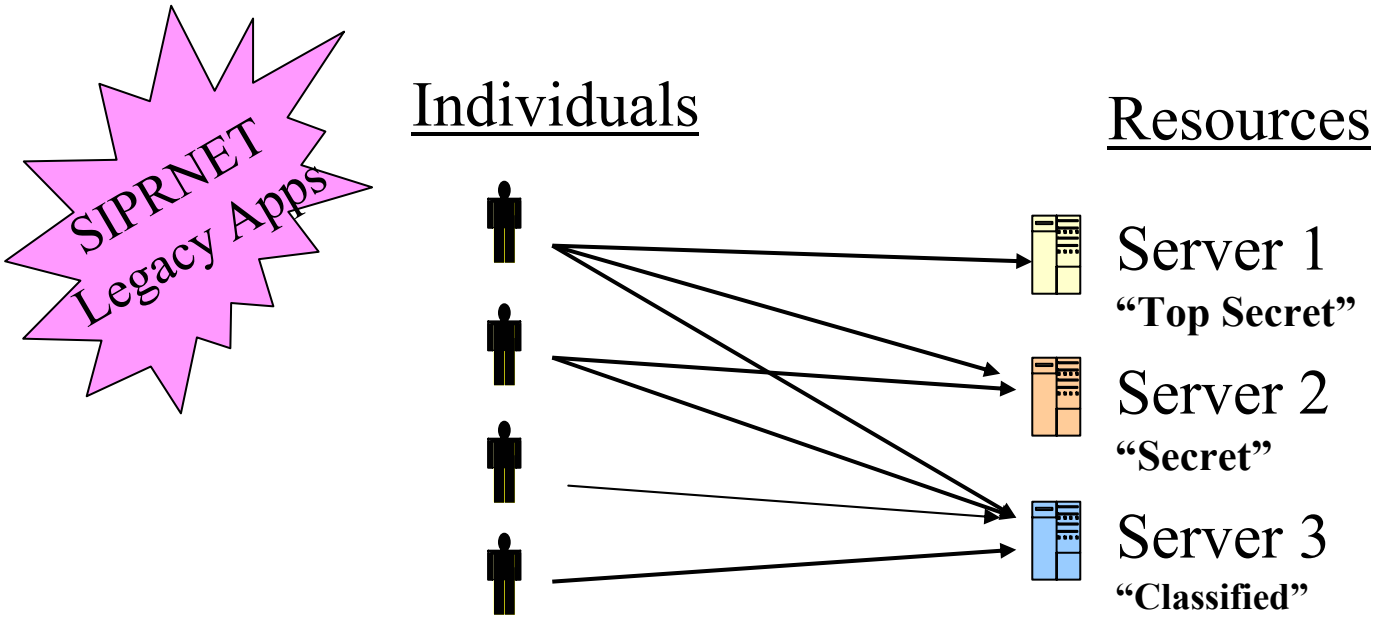
Discretionary AC

Restricts access to objects based solely on the identity of users who are trying to access them.



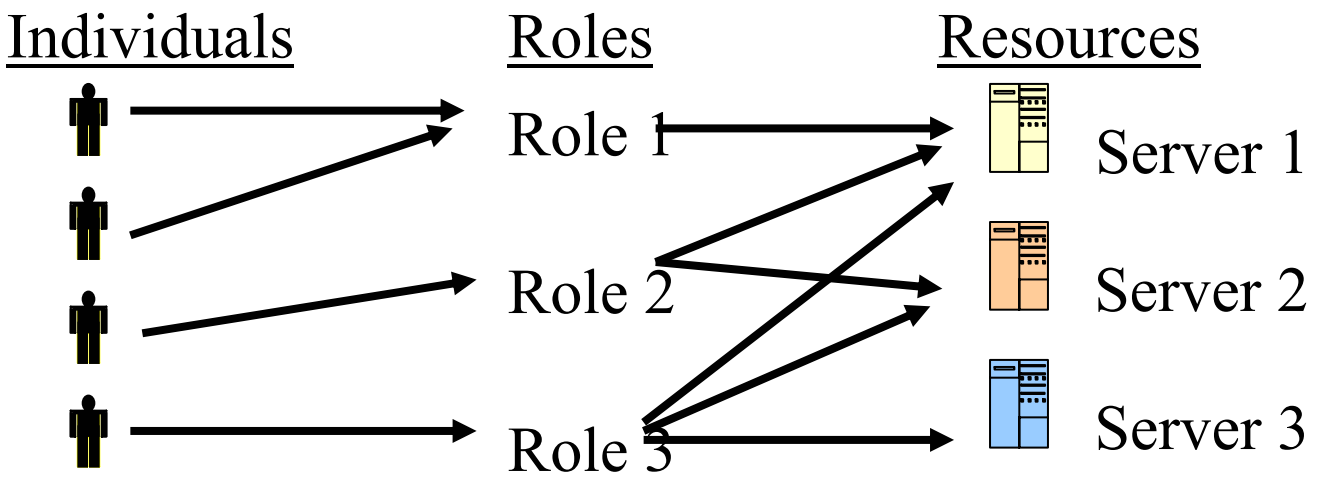
Mandatory AC

Restricts access to data/information based on matching the security level of data being accessed and the identity of the user.



Role-Based AC

Restricts access to data/information based on matching the security level of data being accessed, the identity of the user and the role being performed by the user.



Users change frequently, Roles not as often..

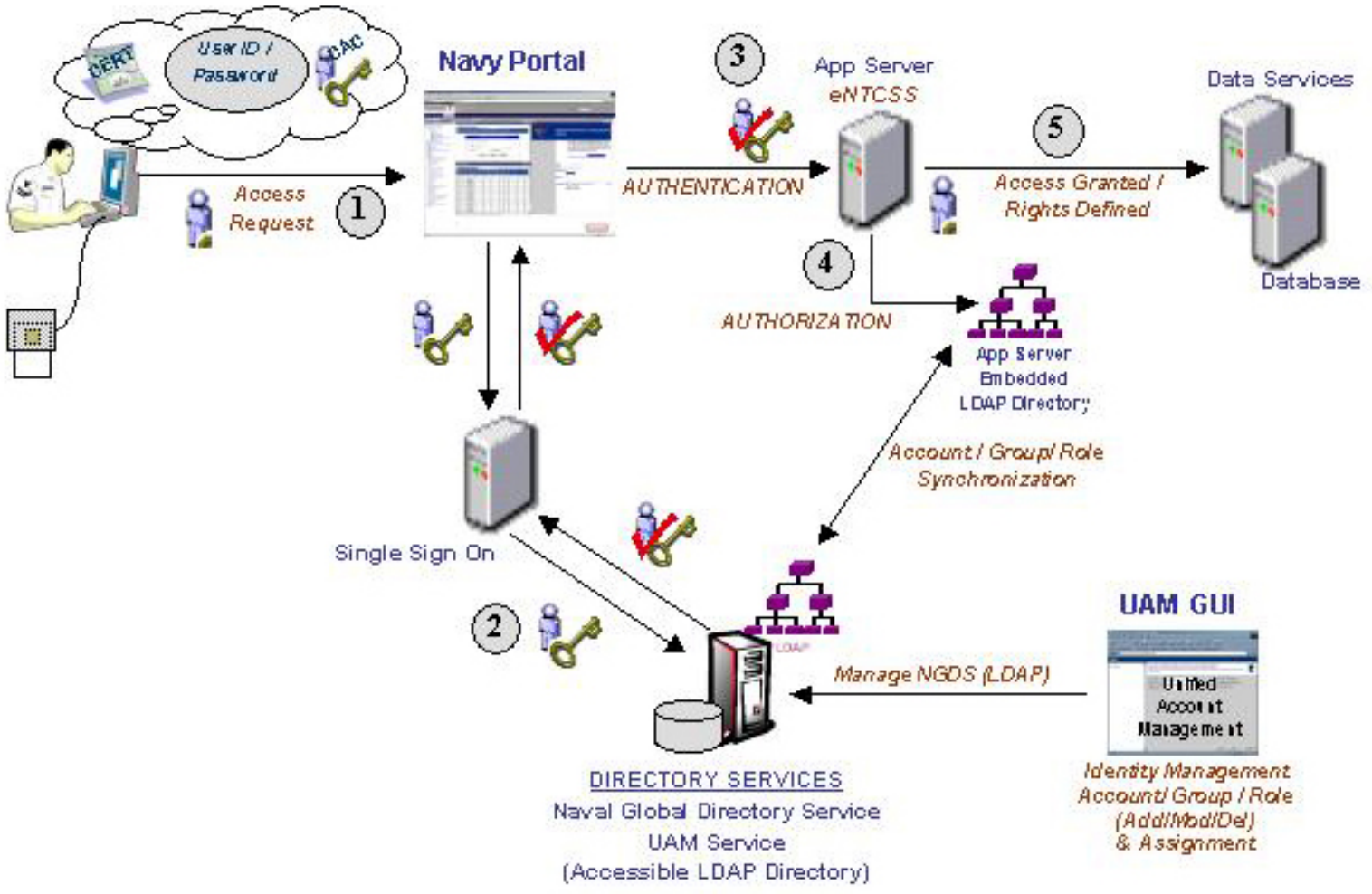
Role Based Access Factors

An Employee-Owned Company

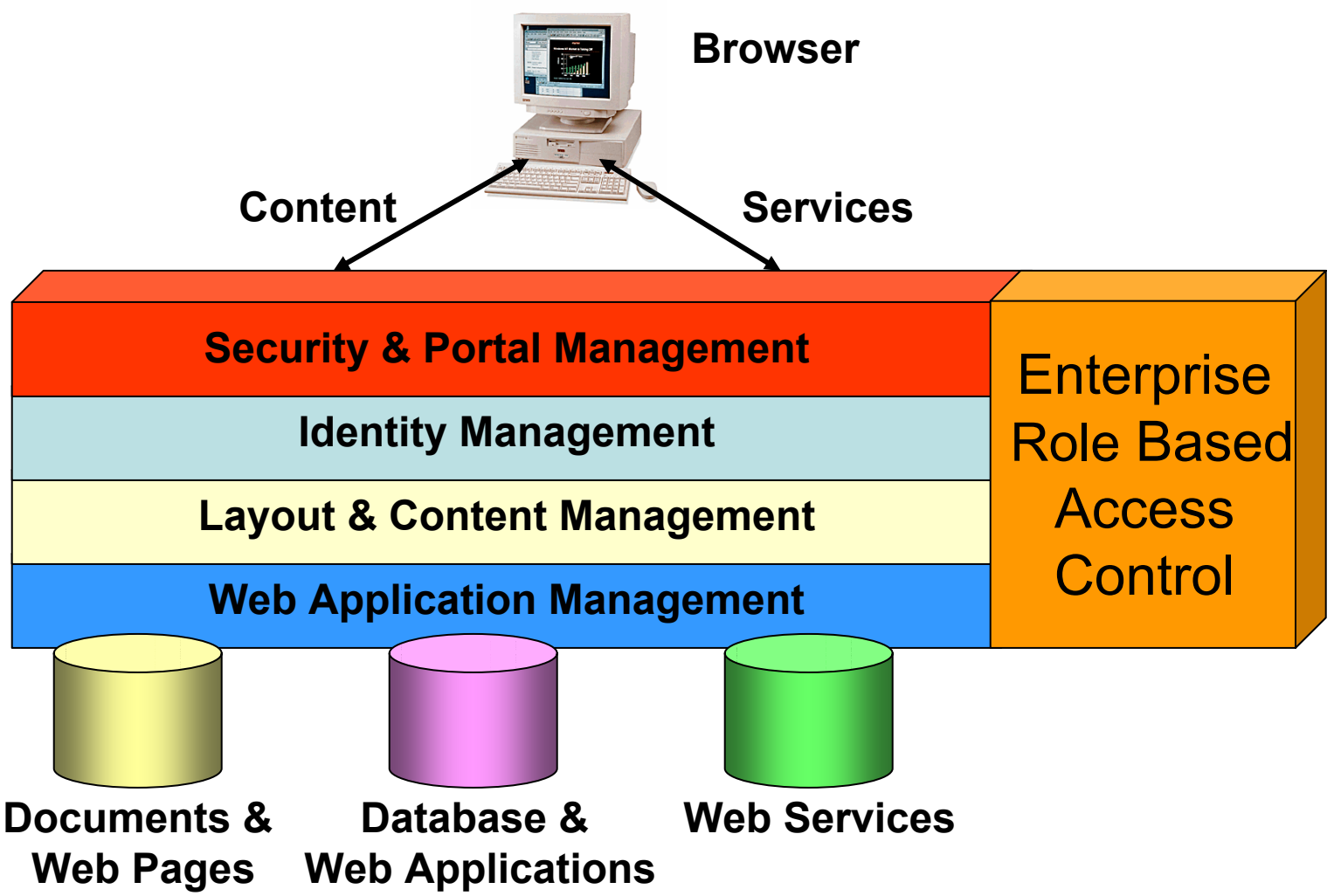
- People
- Functions/processes/rules
  - PMI, SEI-CMMI, BPM
- Data
- Time
- Situation

Access Control Architecture Example

An Employee-Owned Company



Portal/SOA Architectures



Specific Requirements

An Employee-Owned Company

- **Security administration is costly and error prone**
  - 1000's of application access control lists and "forms-based logins"
  - User need to know must be individually determined by app owner
  - "Semi-automated self-sign up registration, email back password" may introduce security risks
  - Rarely are users forced to update USERIDs/passwords
  - There is no process for data/application owners or CDA's to validate access requests from Web services
- **What is needed**
  - Automated, secure, accurate system to 'vet' users by role
  - Flexible role creation and modification
  - Rapid yet completely trustworthy PKI/biometrically enabled Single Sign On
  - Formal enterprise architecture and project, change, and business process management

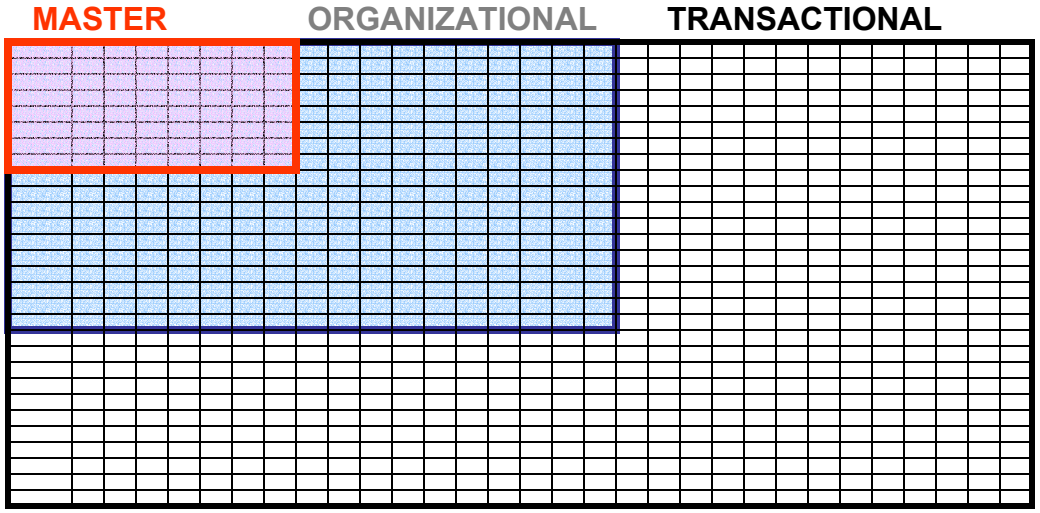
Role Basics ("Rosetta Stone")

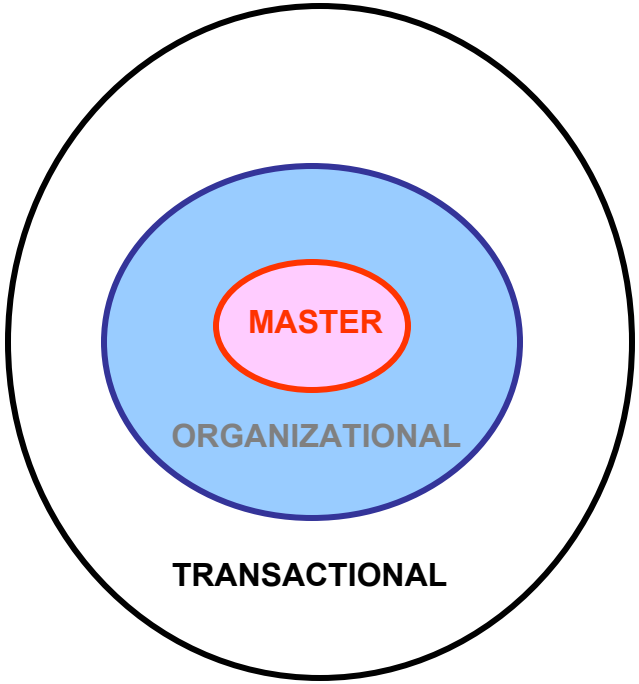
An Employee-Owned Company

Master - Authoritative, objective data objects (name, SSN, DOB, etc.)

Organizational – Local data objects (Command, NEC, Billet, Phone#, etc.)

Transactional – Self input data objects





"VIN" Code

Sample First Digit Choices

A = Active Duty NAVY
B = Reserve NAVY
C = GS
D = Contractor
E = Foreign National
F = Active Duty AF
G= Reserve AF
H=Active Duty ARMY
I= Reserve ARMY
J=Active Duty Marine
K=Reserve Marine
L=Active Duty CG
Etc., etc., etc.,

Essential Provisions of an ERBAC

An Employee-Owned Company

- Should be added to the nine (9) Core Enterprise Services currently listed for NCES
- DoD should fund and maintain a DoD ERBAC office as part of the GIG Enterprise Architecture (EA) effort with an ERBAC representative at every major Joint and Service Echelon 2 and above Command
- Must be one of the major pillars of the Operational portion of the C4ISR Enterprise Architecture (Fn, NCES, etc.)
- Process of defining required roles/policies/rules should be based on a thorough analysis of how the end user operates the system and should include input from all stakeholders

Conclusion

- DoD not realizing promised ROI for IT
- Technology to create an ERBAC system is being implemented today
- ERBAC makes Enterprise Network Centric C2 possible

Next Steps

- Increase DoD wide awareness and actions to resource a solution
- Obtain DoD-wide consensus on ERBAC policy and processes
- Establish a common vocabulary for Role-Based Access Control for use in the DoD Enterprise
- Present a Framework for Role-Based Access Control for both Physical and Virtual Domains

Contact Information

- Rick Kooker

  kookerf@saic.com (808) 833-8661
- Stephan Kane

  kanest@saic.com (808) 833-8658

  3049 Ualena Street, Suite 1100

  Honolulu, HI 96819